REMARKS

I. In the Specification

Amendments to the specification in Applicant's previous Amendment and Response of February 01, 2008 have been rejected under 35 USC §132(a) because the Examiner believes that the amendments add new matter to the specification.

Applicant respectfully submits that for at least the reasons set forth below, *no new matter was added to the specification in the previous Amendment and Response*.

Information regarding "raw" and "sifted" keys

The amendment to the "Background of the Invention" section that clarifies the meaning of the "raw key" and "sifted key" and is basic background information that is known to one skilled in the art. This information is described in the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 2001, in Section 2.3, pages 27-33, which is cited in the "Background of the Invention" section.

No "new matter" is added to the specification when the Applicant simply elaborates on background information already known to those skilled in the art and that is described in a reference cited for its background information.

The definitions of "raw key" and "sifted key" are also *expressly set forth* in the "Detailed Description of the Invention" section of the specification. For example, Applicant's paragraph [0020] reads as follows:

> [0020] With continuing reference to FIG. 1, in the normal operation of a QKD system such as QKD system 10, qubits are exchanged between Alice and Bob by controller 20 causing laser 50 to emit weak (e.g., ~0.1 photon) optical pulses. Controller 20 then provides basis and key bits via TRNG 30 (or alternatively via two separate TRNG's 30) to PM1 to randomly encode the weak pulses. At Bob, controller 120 also causes PM2 to randomly select (via TRNG 120) a basis to measure and detect the modulated qubits at detector 150.

One skilled in the art understands this as constituting the formation of the "raw key."

Applicant's paragraph [0033] and [0034] read as follows.

> [0033] At this point, Bob and Alice run standard QKD procedures (e.g., sifting, error correction, privacy amplification). It is preferable that all information sent during the latter procedures is encrypted with a cipher of the cryptographic strength not lower than the stream cipher. Some information has to be authenticated, as required in the BB84 protocol.

> [0034] Alternatively, Alice and Bob can run sifting and/or error correction first and decrypt the bits afterwards. This would require some simple modifications of decryption process.

The "sifting" procedure referred to in these paragraphs is understood by one skilled in the art to constitute the formation of a "sifted key."

Applicant respectfully submits that for at least these reasons, the Applicant's addition of clarifying language to the "Background of the Invention" section relating to the "raw" and "sifted" keys is both *inherently* an *expressly* supported by the specification and so does not constitute the addition of "new matter" to the specification.

Amendments to independent claims 1, 8 and 9

The Examiner states that language added to independent claims 1, 8 and 9 of "without first forming unencrypted qubits from the optical pulses" is not supported by the specification and constitutes "new matter" added to the Application.

In fact, this limitation is fully supported by Applicant's specification. For example, Applicant's paragraph [0021] and [0023] through [0028] read as follows:

> [0021] However, as discussed above, there are potential security shortcomings in this QKD process. To address these shortcomings, the present invention further involves encrypting (e.g., at the software level) using e/d module **40** at least the key bits from TRNG **30** used to set Alice's phase modulator state for each qubit. This results in "encrypted qubits" being sent to Bob.

[0023] The method of encrypting Alice's key bits is illustrated in FIGS. 2 and 3. Suppose there are b1, b2, . . . bi, . . . bn bits from TRNG 30 for basis and k1, k2, . . . ki, . . . kn bits to form a set of qubits. In an example embodiment, two TRNGs 30 are used to separately generate the basis and key bits, respectively.

[0024] In an example embodiment of the invention, key-bit values k_i are encrypted by e/d module 30 with a stream cipher (e.g., AES in CTR mode). To do this, Bob and Alice must share a pre-agreed password. The stream cipher is needed because some qubits can be lost in quantum channel 200. The loss of qubits during transmission precludes the use of other types of ciphers.

[0025] Suppose Alice and Bob share a password P. In an example embodiment, password P is created by either using a fraction of their key generated by QKD. In another example embodiment, password P is created using one of the known method, such as secure currier or Diffie-Hellman protocol. In an example embodiment, Alice and Bob agree to refresh the password P at a chosen rate. Having this password, they can generate a pad p1, p2, . . . pi, . . . pn by means of a stream cipher

[0026] Once the pad is generated, Alice then performs in e/d module 30 the "exclusive OR" (XOR) operation:

[0027] ki XOR pi=ci

[0028] Alice also sets her phase modulator PM1 to encode ci on a qubit, not ki. This process is illustrated in the flow diagram of FIG. 3. The result is what is referred to herein as an "encrypted qubit" or an "encoded qubit."

One skilled in the art understands that these paragraphs describe in detail what is summarized in the aforementioned claim amendment language, namely, that ***Alice never forms an unencrypted qubit.***

As one skilled in the art further understands, a qubit is not formed until the optical pulse is modulated. Since the first modulation in Applicant's invention occurs with an encrypted modulation, the result is an encrypted qubit without having formed an unencrypted qubit.

Accordingly, the amended language for claims 1, 8 and 9 is fully supported by the specification in at least the paragraphs cited above and so does not constitute "new matter."

Amendment to independent claim 5

The Examiner also objects to the amendment to claim 5 that adds the limitation "simultaneously so as to simultaneously encoded {*sic*: encode} and encrypt the optical pulses to form encrypted qubits" and asserts that this constitutes "new matter" that must be canceled.

Applicant respectfully disagrees with the Examiner. With reference to the above-cited paragraphs [0021] and [0023]-[0028], one skilled in the art understands from this enabling disclosure that the encoding of the optical pulse and the encrypting of the optical pulse occur simultaneously through the use of the encrypted key bits.

Accordingly, the amended language for claim 5 is fully supported by the specification in at least the above-cited paragraphs and so does not constitute "new matter."

In view of the above reasons, Applicant respectfully requests the withdrawal of the objection to the above-cited amendments to the specification and claims.

In the Claims

Claims 1-13 are pending in the application stand rejected.

Claim 5 has been amended to correct a typographical error.

Claim 10 as been amended to correct the dependency of this claim from itself to claim 8 as kindly pointed out by the Examiner.

I. Claim rejection under 35 USC § 112

Claims 1-4 and 8-13 stand rejected under 35 USC §112, first paragraph, as failing to comply with the written description requirement and for not being enabled.

For at least the reasons discussed above in connection with the objections under 35 USC § 132(a) to the amendments to the specification and claims made in the previous Amendment and Response for being "new matter," Applicant respectfully submits that the amendments to claims 1, 5, 8 and 9 are fully supported by the written description and enablement provided in at least paragraphs [0020] through [0028] of Applicant's specification.

Applicant therefore respectfully requests withdrawal of the rejections under 35 USC §112, first paragraph, of the above-cited claims for failure to satisfy the written description and enablement requirements.

II. Rejections under 35 USC §103

Claims 1 and 9 were rejected over U.S. Patent No. 5,757,912 to Blow ("Blow") in view of U.S. Patent Application Publication No. 2004/0032954 to Bonfrate et al. ("Bonfrate").

An obvious rejection under 35 USC §103(a) requires that the combination of cited references yield all of the claim limitations. Also, the claim must be *read as a whole* to avoid the impermissible assembling bits and pieces of prior art to reconstruct Applicant's claimed invention using hindsight.

Claims 1-4

The Examiner correctly points out that Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits. The Examiner then asserts that "Bonfrate discloses encoding key information and having single optical photons (qubits) [that] carry said encoded key information" (citing Bonfrate paragraph [0007]). This statement stands for the usual prior art proposition that photons are encoded via phase modulation in order to form encoded (but unencrypted) qubits tha form an encrypted key. This *encoding* is *not the same* as using *encrypted key bits* to form *encrypted* qubits.

A closer reading of Bonfrate reveals that Bonfrate has nothing to do with forming encrypted qubits in the manner claimed by Applicant. Bonfrate discloses a quantum cryptography apparatus that "overcomes problems associated with polarisation evolution in quantum cryptography systems that incorporate a non-polarisation preserving optical channel (e.g., standard optical fiber)." See Abstract. Bonfrate does this by avoiding the use of an active random number generator and phase modulator at the receiver by using a polarization beam splitter (**14**) that serves as a random router. Paragraph [0029]; FIG. 1. The *encoding* performed by Bonfrate is the usual polarization encoding used to form *unencrypted qubits*. It has nothing to do with forming *encrypted qubits* per Applicant's claimed invention.

There is absolutely no teaching or suggestion in Bonfrate of forming encrypted qubits using encrypted key bits. Therefore, the combination of Blow and Bonfrate does not yield all of the limitations in Applicant's claim 1. Consequently, a *prima facie* case for obviousness cannot be established using these references.

The obviousness rejection of Applicant's claim 1 is therefore traversed and withdrawal of the rejection is earnestly requested. For the same reasons, the obviousness rejection as applied to dependent claims 2-4 is also traversed and withdrawal of the obviousness rejection of these claims is earnestly requested.

Claims 5-7

Claim 5 is rejected for the same reasons as claim 1, and further in view of the article "Applied Cryptography" by Schneier ("Schneier"). Accordingly, the rejection of claim 5 and its dependent claims 6 and 7 is traversed for the same reasons set forth above in connection with the obviousness rejection of claims 1-4.

Claim 8-13

Claims 8-13 are rejected under 35 USC §103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend ("Townsend") in view of U.S. Patent Application Publication No. 2006/0120529 to Gisen et al. ("Gisen"), and further in view of Schneier and Bonfrate.

Applicant reiterates here that a closer Bonfrate reveals that Bonfrate has nothing to do with forming encrypted qubits in the manner claimed by Applicant. Bonfrate discloses a quantum cryptography apparatus that "overcomes problems associated with polarisation evolution in quantum cryptography systems that incorporate a non-polarisation preserving optical channel (e.g., standard optical fiber)." See Abstract. Bonfrate does this by avoiding the use of an active random number generator and phase modulator at the receiver by using a polarization beam splitter (**14**) that serves as a random router. Paragraph [0029]; FIG. 1. The *encoding* performed by Bonfrate is the usual polarization encoding used to form *unencrypted qubits*. It has nothing to do with forming *encrypted qubits* per Applicant's claimed invention.

The cited references and the arguments set forth by the Examiner indicate that the Examiner is not reading each claim *as a whole* to appreciate and understand the invention *in its entirety*. The Examiner seems to have fallen into the trap of using the claims as a guide to find references covering different features of the invention without regard to what the invention covers *as a whole*. This is impermissible hindsight reconstruction of the claims using the prior art. See, e.g., *In re Fritch*, 972 F.2d 1260, 23 USPQ 2d 1780, 1784 (Fed. Cir. 1992).

11

All of the cited patent references are directed to the conventional practice of quantum key distribution (QKD) that involved the random modulation of optical pulses to form unencrypted qubits. The Schneier reference is directed to classical encryption, and Applicant's invention admits to using classical encryption since it is invention is entitled "QKD with classical bit encryption." However, it is the **combination of claim elements taken as a whole** that combine classical encryption with quantum cryptography in **a unique and non-obvious way** to provide enhanced security over existing quantum encryption systems.

There is absolutely no teaching, suggestion or motivation in any of the cited references to form encrypted qubits using encrypted key bits in the manner claimed by the Applicant. Moreover, the combination of the cited references does not yield all of the limitations in Applicant's claims 8-13. Consequently, a *prima facie* case for obviousness cannot be established using the cited references.
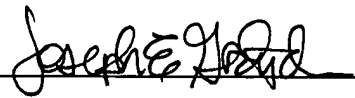
Accordingly, the obviousness rejection of Applicant's claims 8-13 is traversed and withdrawal of the rejection is earnestly requested.

CONCLUSION

Applicant respectfully submits that claims 1-13 as presently presented are in condition for allowance.

The Examiner is encouraged to contact the Assignee's authorized representative at 941-378-2744 to discuss any questions that may arise in connection with this Amendment.

Respectfully Submitted,

By: _____ Date: <u>May 30, 2008</u>
Joseph E. Gortych
Reg. No. 41,791

Customer No. 53590

Opticus IP Law PLLC
7791 Alister Mackenzie Dr
Sarasota, FL 34240 USA

Phone: 941-378-2744
Fax: 321-256-5100
E-mail: jg@opticus-ip.com